pursuit
WEALTH PLANNING

Watch out for Scammers

When was the last time you received a phone call or email from a scammer? If you were contacted recently, you aren't alone.

Internet scams show no signs of letting up. In fact, the problem may be getting worse. In its most recent report from the [[https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 Internet Crime Complaint Center (IC3)]], the FBI said it saw the largest number of complaints and the highest dollar losses reported since the center was established 20 years ago.

The FBI said it recorded 467,361 complaints in 2019 and more than $3.5 billion in losses to individuals and businesses.

The costliest scams involved business email compromise, romance or confidence fraud, and mimicking the account of a person or vendor known to the victim to gather personal or financial information, the FBI said.

"Criminals are getting so sophisticated," Donna Gregory, the chief of IC3 said. "It is getting harder and harder for victims to spot the red flags and tell real from fake."

But you can avoid becoming a victim with vigilance and common-sense steps.

1. **Beware of the fake invoice or suspicious email**. Be sure to check that email address. The name may be familiar, but the email address may be a long string of unrelated characters. Other scamsters may have an email that is one letter off. Or they may simply use .net instead of .com.

   Does an invoice ask you to provide new bank information? That's a potential red flag. A simple way to side-step a fraudulent transfer of funds is to verify you are using a trusted source, for instance making a quick phone call to the vender. If you are business owner, require your employees to call and verify payment requests using phone numbers that are on file.

2. **Scammers will pretend to be from an institution you are familiar with**. You've probably received these emails or phone calls. Someone reaches out to you claiming to be from the IRS, the Social Security Administration, or another government organization. The caller says you owe money and that you must pay, or legal action will be taken.

   The email may have official logos, or your caller ID may reflect the government agency's name.

Let me be clear on this. The IRS will ***never*** make first contact via a phone call and claim you owe them money. You'll receive a letter with details and steps you can take. *If you receive a call, simply hang up the phone*. Please do not engage the caller. Some may threaten or become abusive.

If you "settle" and pay over the phone, expect repeated phone calls as more "discrepancies" are found. In other words, they will extract as much cash as you allow them too.

3. **Avoid the Social Security scam**. In one version of the scam, the caller says your Social Security number has been linked to a crime involving drugs or sending money out of the country illegally. They then tell you that your Social Security number is blocked. For a fee, it can be reactivated. Then the scammer will ask you to confirm your Social Security number.

   Hang up. The Social Security Administration will ***never*** call you on the phone and ask for your Social Security number.

4. **Scammers will tell you how to pay.** They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back.

   Others will send you a check (that will later turn out to be fake), tell you to deposit it, and then send them money. This is a common Craigslist scam. The caller wants to purchase your items sight unseen. Or they will want you to set up a PayPal account or some other type of electronic payment. (On the other hand, if you are selling items, cash is usually the best way to proceed.)

5. **Pop-up warnings**. Tech support scammers may try to lure you with a pop-up window that appears on your computer screen. It might look like an error message from your operating system or antivirus software. It might use logos from trusted companies or websites.

   The message in the window warns of a security issue on your computer and directs you to call a phone number to get help. Simply ignore. You can always use your antivirus software to scan.

   If you call, they'll likely give you worthless information--for a fee. They may also have you download malware or other unwanted software that they claim will fix the issue.

6. **Avoid phishing scams**. [[https://www.phishing.org/what-is-phishing Phishing]] is a cybercrime in which a person is contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as banking, credit card details and passwords.

   Phishing emails and text messages spin a tale in order to trick you into clicking on a link or opening an attachment.

   For example, they may:

- Claim they've noticed some suspicious activity or log-in attempts
- Claim there's a problem with your account or your payment information
- Say you must confirm some personal information
- Include a fake invoice
- Want you to click on a link to make a payment
- Say you're eligible to register for a government refund
- Offer a coupon for free items

Here is one example from the Federal Trade Commission (FTC): You may receive an email that appears to be from a company you are familiar with, such as Netflix. Not everyone subscribes to Netflix, but tens of millions do.

You receive the email requiring that you update credit card or bank information for payment. If you comply, you've given criminals personal information they can use to steal from you. (If you are unsure, go to the website of the company and check your information there.)

Also be careful about clicking on links or attachments that could compromise your personal information or lock up your computer. Use these four steps to protect yourself from phishing:

- Use updated virus protection software and keep your browsers and operating system updated.
- Protect your mobile phone by setting software to update automatically.
- Protect your data by backing it up.
- Protect your accounts by using multifactor authentication, which simply means you will get a text or email with a passcode when you log into an account.

  Please note that some of these email/texts now include a warning not to give out the passcode to anyone. Why is this needed? Some scammers will attempt to log into your account, then call claiming they are from that company and need your passcode. Just hang up.

7. **Steer clear of the fake Facebook page**. Scammers sometimes set up a fake Facebook page of a well-known company. Scammers then add a post claiming they will give away autos, free airline tickets, or thousands of dollars to "hundreds of lucky winners." Simply share the post, comment, click on a provided link, and fill out the requested information.

   If you look at the FB page, you'll notice it's brand new as there are few posts, and it lacks a verified FB badge indicating its authenticity. However, you'll see hundreds of individuals who have dutifully complied with the scammer's requirements. Sadly, they will win nothing but grief.

What to do if you are scammed

Be vigilant and use common sense. Anyone can fall victim to these scams. If you have paid someone, call your bank, money transfer app, or credit card company and see if they can reverse the charges.

If you gave personal information, go to [[https://www.IdentityTheft.gov IdentityTheft.gov]] to see what steps you should take, including how to monitor your credit.

Did a scammer take control of your cell phone number and account? Contact your service provider to take back control of your phone number. Once you do, change your account password. Passwords should be lengthy and include numbers, letters, special characters, and capitalized letters. Short passwords can easily be hacked using computer programs.

When you report a scam, the FTC can use the information to build cases against scammers, spot trends, educate the public, and share data about what is happening in your community. If you were scammed, report it to the FTC at ReportFraud.ftc.gov.

Finally, be vigilant and use common sense. Avoid clicking on suspicious links, and never give out personal information to a stranger over the phone. You'd never tell your best friend your annual income, so why would you give a suspicious caller your passwords, bank information, date of birth or your Social Security number.

Sources and further reading

- [[https://www.consumer.ftc.gov/articles/how-avoid-scam How to avoid a scam]]
- [[https://www.consumer.ftc.gov/articles/what-do-if-you-were-scammed What to do if you were scammed]]
- [[https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams How to recognize and avoid phishing scams]]
- [[https://www.consumer.ftc.gov/blog/2018/12/fake-calls-about-your-ssn Fake calls about your SSN]]
- [[https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams How to spot, avoid and report tech support scams]]